IT CHECKLIST FOR UK LAW FIRMS

A practical, security-first IT checklist for UK law firms

Prepared by
Computer Support Centre
https://computersupportcentre.com

IT Checklist for UK Law Firms

Executive summary

- Law Firms Don't Need "Enterprise Everything" But Require CONSISTENT, DOCUMENTED "Confidentiality-First" IT.
- Most Major Cyber-Emergencies Start With Email (Phishing, Mailbox Rules, or Fake Invoice Change).
- Weak Access Control is Also Harmful.
- A Baseline For Documenting Data Protection Needs To Protect The Confidentiality, Integrity, And Availability Of Client Data. It Needs To Show That You Have Taken Reasonable Steps In Protecting Data.
- Maintain Separate Admin Accounts, Multi-Factor Authentication (MFA), and Lock Down Email Domains (SPF/DKIM/DMARC), HIGH IMPACT, LOW DRAMA
- A Good Document Management Strategy Prevents Case Files From Being Scattered Across The World: Choose One System Of Record (DMS/SharePoint) And Enforce Permissions Discipline.
- Backups Are About Being Able To Restore An Environment, Not Just Having Backups. You Need To Assume You Will Have A Ransomware Attack, You Should Test Restores And Protect Backups From Ransomware Attacks.
- Prepare An Incident Pack That Includes Initial Steps And Evidence Checklist And A Contact Tree. It Will Reduce The Likelihood Of Action Panic And Mistakes.
- Create A Minimum Level Baseline In 30 Days, Then Quarterly Improvements.

Who this guide is for

This guide is designed for:

- UK-based law firms of all sizes ranging from one-person show to approx. 100 employees.
- All levels of leadership including: managing partners, compliance officers, operations leaders.
- Firms that utilise standard application stack systems such as: Microsoft 365, case/practice management systems; DMSs/e-Sign; Scanning; Dictation tools.

Who it isn’t for

- Large corporate multi-national law firms who have their own internal security teams managing a complex environment of multiple bespoke and in-house built applications.
- Law firms requiring legal opinions about the interpretation of regulations; What is the threshold for reporting and how long must retention take place.
- Very specialised sectors where the only compliance framework is specific to that sector and requires other forms of compliance advice.

Disclaimer (important)

This guide is for your reference and greater understanding of an operational approach. It should not be construed as a legal opinion or as an interpretation of SRA regulatory/operational rules or of

Data Protection legislation in relation to your individual situation(s). If you are unsure of any regulatory issues affecting you or your organisation, you should obtain appropriate professional assistance (there is a general reference to confidentiality obligations/expectations that the SRA has for its members).

One-page "Minimum Secure IT Baseline for Law Firms"

If you need a yes/no answer here, start from this list.

Accounts & Access	Devices
✓ Use only named user accounts ✓ Enable MFA for all email accounts ✓ Create separate admin accounts ✓ Use a joiner/leaver checklist when adding a new employee	✓ All laptops/desktops must be encrypted ✓ Only support currently supported operating systems ✓ Software updates must be enabled and documented at least once a year. ✓ Screen locks must be enabled, and there must be a strong password/PIN policy.
Email & Fraud Prevention	**Data & Documents**
✓ Enable SPF/DKIM/DMARC to decrease the amount of email being spoofed. ✓ Enable anti-phishing protection, and ensure there is a user reporting button. ✓ Have an established process for changing payment details that involves a callback verification step.	✓ All matter documents must be stored in one of the approved Document Management Systems. ✓ Access to document will be controlled by role and/or matter team. ✓ Each firm must not store client files on any uncontrolled, unmonitored, or unsecure local storage system.
Backup & Recovery	**Monitoring & Incident Response**
✓ Backup critical systems and cloud data where necessary. ✓ Document the results of the annual restore test. ✓ Backup access protected from ransomware	✓ Ensure there is a centrally managed endpoint protection / anti-virus solution in place. ✓ Create an incident checklist for the first 60 minutes of an incident occurring. ✓ Staff get basic cyber/confidentiality awareness refresh

1) Governance & accountability

Why it matters for law firms

IT is an essential component of law firms that it does not just support the provision of services to clients; it is a vital aspect of maintaining the safety, integrity and confidentiality of client information, thus maintaining the firm's service offering. The Security Regulatory Authority (SRA) requires firms to take adequate measures to both protect their client's data and maintain confidentiality.

Item	Minimum	Better	Best practice	Owner	Frequency	Note
IT ownership	manager	IT & risk owner pair	Board-level oversight	Practice Mgr	Ongoing	Someone accountable
Policies	Basic set	Reviewed annually	Tested + versioned	COLP/Ops/ IT	Annual	Short & usable
Risk register	Informal list	Simple risk log	Reviewed quarterly	COLP/COF A	Quarterly	Include cyber/fraud
Documentation	Minimal	Central repository	Maintained run-books	IT	Quarterly	How to restore

Common pitfalls

- No single owner for IT risk (especially in multi-partner firms)
- Policies exist but no one is following them
- No Written process for how to handle incidents/leavers

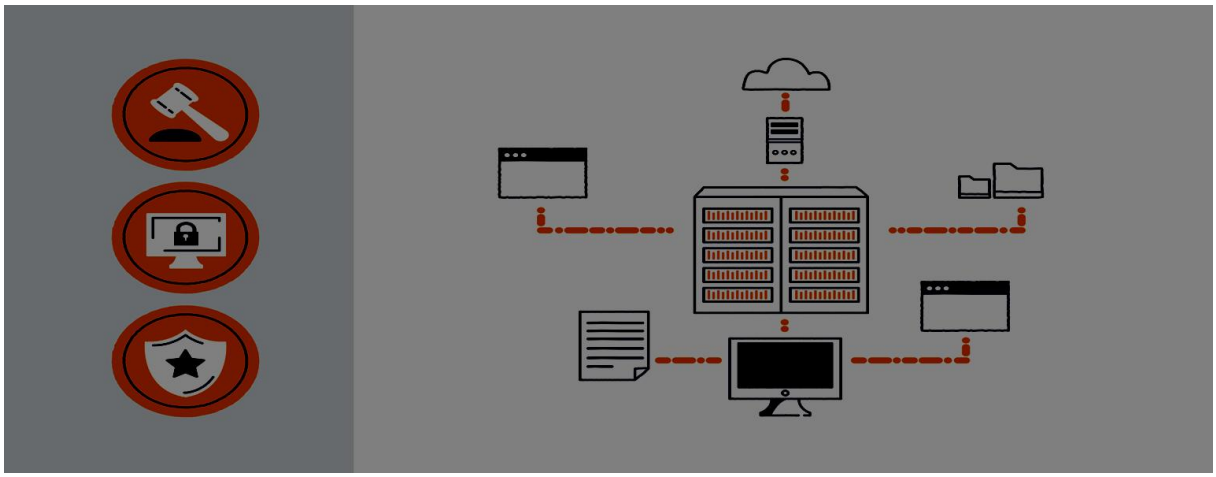
Quick wins

- Appoint an accountable owner (even if you have outsourced IT Support)
- Create a one-page "IT Risk Dashboard" (MFA, Backups, Patching, Incidents)
- Create a central documentation folder and password vault

2) Devices & endpoints

Why it matters for law firms

The use of lost or stolen laptops, outdated PCs and unmanaged devices are common causes of confidentiality breaches and systems downtime. The Guidance on Cyber Security published by the Law Society highlights the need to have measures in place to protect the client’s data from loss or unauthorised access.



Item	Minimum	Better	Best practice	Owner	Frequency	Note
Device standard	Any business device	Approved models list	Standardised fleet	IT/Ops	Annual	Easier support
Encryption	Recommended	Enabled	Enforced + escrow keys	IT	Ongoing	BitLocker/ FileVault
Endpoint control	Local admin common	Limited admin	Managed device policies	IT	Quarterly	Reduce risk
Lifecycle	Replace on failure	4–5 years planned	3–4 years planned	Finance	Annual	Budget line

Common pitfalls

- Utilising Personal Devices for Case Work with no safeguards in place
- Laptops with no encryption
- Devices have Run-Out-of-Support Operating Systems
- Old Hard Drives are being kept in cupboards.

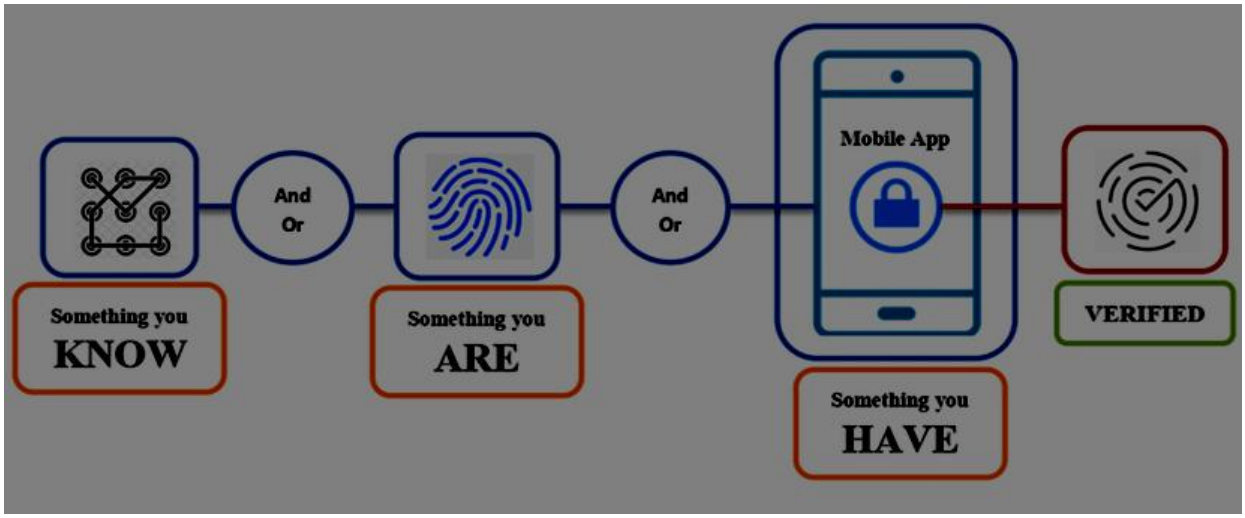
Quick wins

- Turn on BitLocker / FileVault for All Laptop Hard Drives
- Remove Local Administrator Rights when possible
- Create an Asset Register (Owner, Serial Number, Encryption Status).

3) Identity & access control

Why it matters for law firms

Cybercriminals are increasingly accessing computer systems with stolen usernames and passwords, and Adopting access controls will help protect the confidentiality of client communications and mitigate internal mistakes of providing access to matters (wrong matters).



Item	Minimum	Better	Best practice	Owner	Frequency	Note
User accounts	Named accounts	Role-based groups	Least privilege enforced	IT	Ongoing	No shared logins
MFA	Admins only	All users	Conditional access	IT	Annual	Especially email
Admin separation	Mixed use	Separate admin accounts	Just-in-time admin	IT	Quarterly	Reduce Global Admin
Leavers	Manual	Checklist	Same-day automated	HR/IT	Per leaver	Highest risk gap

Common pitfalls

- Shared accounts, e.g., "Reception@," "Accounts@"
- Access to accounts from former employees
- Too many users with Global Admin access
- Partners wanting to get around control, "quick and easy"

Quick wins

- MFA Applies to All Accounts (Begin with Email)
- Administrative Users Verified and Restricted
- Enable all highlighted Security Leaver Process

4) Email & communications security

Why it matters for law firms

Email is the primary method that cybercriminals use to perpetrate phishing scams, property fraud, and impersonation of law firms (or their clients), and therefore, ensuring client communication is protected will meet client expectations surrounding confidentiality and upholding the standards of care.

Item	Minimum	Better	Best practice	Owner	Frequency	Note
Email platform	Business email	M365/Google hardened	Advanced threat protection	IT	Annual	Avoid free email
Domain protection	SPF	SPF+DKIM	SPF+DKIM+DMARC	IT/DNS owner	Annual	Reduces spoofing
Phishing controls	Default filtering	Anti-phish policies	Managed tuning + alerts	IT	Monthly	Review quarantines
Secure comms	“Email only”	Encrypted option	Client portal/secure share	Ops/Partners	Annual	Sensitive matters

Common pitfalls

- No enforcement of DMARC makes spoofing simple
- Email is relied upon for Bank Account Changes, without verification
- Weak shared mailbox permissions
- No method for reporting suspicious emails

Quick wins

- Add DMARC (start with a monitoring Policy and slowly tighten)
- Create a "Report Phishing" button for staff and provide them with instructions
- Establish a procedure for verifying changes to how payments are made via phone

5) Practice management & legal software

Why it matters for law firms

A Case Management System holds the most valuable data of an assn: A case management system can be composed of the Crown Jewels of an association, including; client identification, case files, case documentation, financial tracking, and periodically, due diligence on Anti-Money Laundering evidence. It is imperative to properly control vendor access and have a mechanism to regularly patch the system.

Item	Minimum	Better	Best practice	Owner	Frequency	Note
Access control	Basic roles	Role review	Matter-based controls	Practice Mgr/IT	Quarterly	Least privilege
Updates	Ad-hoc	Scheduled	Tested change windows	IT	Monthly/Quarterly	Avoid surprises
Vendor risk	Contract only	Access documented	Annual vendor review	Ops/COLP	Annual	Who can access data?

Common pitfalls

- Vendors with unmonitored administrative access
- Old vulnerabilities (with associated older versions of software/operating system)
- Over-permissioned users (such as saying, “Everybody is a Supervisor”)
- Lack of identifiable storage/back-up location of data

Quick wins

- Document: hosting model, support access, backup responsibilities
- Review who has “superuser” roles
- Align update schedule with business hours

6) Data storage & document management

Why it matters for law firms

Special category data and confidential information and other sensitive client files have high-level permissions set up and clear “system of record” in place, reducing the chance of accidental disclosure.

Item	Minimum	Better	Best practice	Owner	Frequency	Note
System of record	Mixed locations	Defined DMS/SharePoint	Controlled DMS + policy	Partners/IT	Annual	Stop sprawl
Permissions	Shared drives	Matter/team-based	Reviewed + audited	Matter owners/IT	Quarterly	Least privilege
External sharing	Allowed	Restricted	Approved workflow	IT/Compliance	Quarterly	Track sharing links
Version control	Ad-hoc	Standard tool	DMS controls	IT	Ongoing	Reduce confusion

Common pitfalls

- Matter folders saved to a desktop (or USB) drive can be accessed by anyone with access to that drive.
- Folders that are shared externally will not expire unless deleted by the originator.
- There is confusion around whether documents should be stored in OneDrive (personal) or SharePoint (the firm).

Quick wins

- Determine the location where all Matter Documents should reside.
- Restrict the ability for people to share Matter Documents externally to only those approved by management.
- Run a permission review of the top ten most sensitive Matter Folders.

7) Backups & disaster recovery

Why it matters for law firms

Backup serves as an overarching safety feature for Defending against Ransomware Attacks / Deletion / Suppliers. In the context of protecting Confidentially, Integrity, and Availability in your firm's Legal Work.

Item	Minimum	Better	Best practice	Owner	Frequency	Note
Backup coverage	Key files	Files + systems	Full environment + SaaS	IT/MSP	Annual	Include PMS/DMS
Approach	Single copy	3-2-1	Immutable + 3-2-1	IT/MSP	Ongoing	Protect from ransomware
Testing	Never	Annual restore test	Quarterly restore tests	IT/MSP	Quarterly	Document results

Common pitfalls

- Cloud Doesn't Necessarily Mean Backed Up
- Backup Access With Same Administrator Credentials (ransomware access risk)
- No Testing of Restores
- No Clear Recovery Time Goals

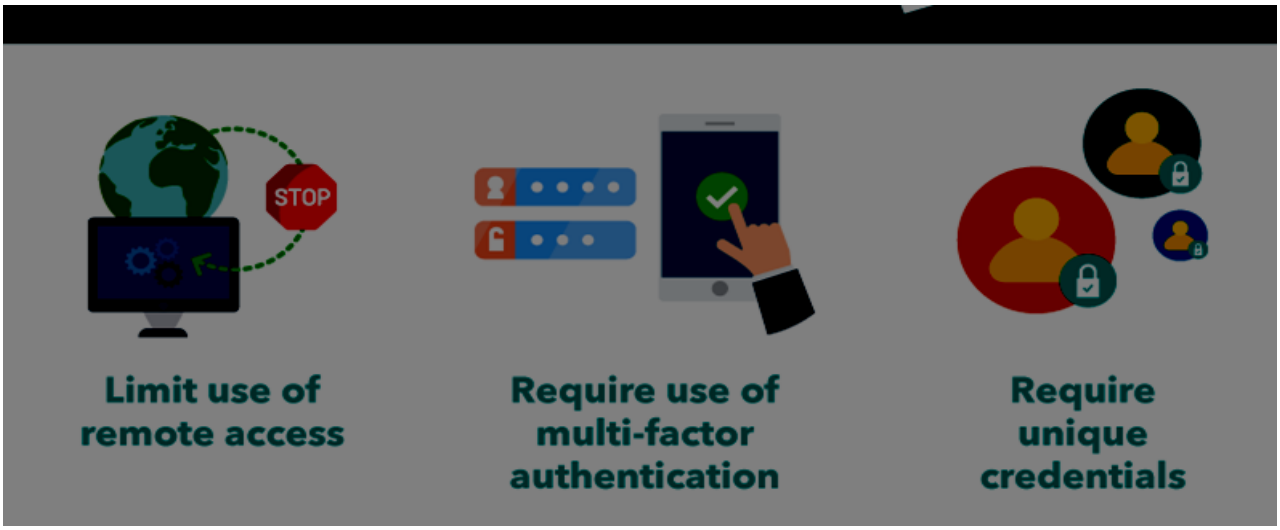
Quick wins

- This week, test restoring a folder containing information that pertains to one of your matters.
- Backup should be stored on separate administrator credentials and/or on Immutable storage whenever possible.
- Create a one-paged Disaster Recovery Priority List.

8) Remote & hybrid working

Why it matters for law firms

Working remotely exposes workers (via their home networks, shared spaces within their homes, as well as their own devices); however, implementing policies and processes around working from home can lead to effective security when properly structured and planned.



Item	Minimum	Better	Best practice	Owner	Frequency	Note
Remote access	VPN	VPN + MFA	Zero-trust access	IT	Annual	No exposed RDP
Device policy	Informal	Written	Enforced via MDM	Ops/IT	Annual	BYOD rules
Home working	No guidance	Basic checklist	Minimum standards	Ops	Annual	Privacy/screens
Mobile security	PIN	Remote wipe	Managed mobiles	IT	Ongoing	Lost phone risk

Common pitfalls

- Storing Important Case Files on Your Personal Computer
- Printing documents from home without any sort of controls being in place
- Saving Passwords in Web Browsers on Unprotected Devices
- Accessing Email through Your Unsecured Phone

Quick wins

- Implementing the Use of Encryption with Multi-Factor Authentication for Each Device Used Remotely to Access Company Data.
- Developing a 1-Page Secure Home Working Guide
- Prohibiting Automatic Synchronisation for Any Sensitive Libraries to Unprotected Devices Whenever Possible.

Common risks & failure points (law-firm specific)

- Fraudulent conveyancing payments (use of fake invoices or Bank Transfer details)
- Compromised mailboxes (via unknown rules inside their mailbox or OAuth abuse)
- E-mail (hijacking) and spoofing (not being able to identify a partner’s email address)
- Case files being too widely shared (someone internally could have accessed them accidentally)
- Unencrypted laptops used in court or for meetings
- Companies employing ineffective procedures to secure former employees
- Outdated, unsupported technology used to manage cases
- Failure to test back up systems until they become necessary
- Supplier access creep (multiple suppliers with the authority to perform administrator functions)
- No documentation of incidents for potential improvement and assessment of the event's scope.

30-day improvement plan (Week 1–4)

Week 1: Employee Visibility and Immediate Risks
✓ Identify the Users, Devices, and Admin for Your Organisation ✓ Set Up Multi-Factor Authentication (MFA) for All Employees (starting with email) ✓ Identify and develop a plan to eliminate any Shared Accounts ✓ Verify the Encryption Status of All Employees' Laptops
Week 2: Email Fraud Prevention
✓ Set Up/Update Security Protocols for Email (SPF/DKIM/DMARC) ✓ Create a Phishing Attack Prevention and Reporting Process ✓ Create a Method for Employees to Call to Verify Payment Changes ✓ Review All Employees' Access and Permission Levels to Shared Mailboxes
Week 3: Protecting Company Data and the Backups
✓ Define the Company's System of Record for Project Documentation ✓ Create a Policy to Restrict External Sharing of Company Data ✓ Verify Backups and Conduct a Test Restore of the Backups ✓ Document the Company's Disaster Recovery Plan and the Five Most Critical Systems
Week 4: Monitor Incidents and Prepare for Incident Response
✓ Verify End-User Protection Procedures in Place/Incident Alerting Procedures ✓ Document the Company's Regular Resilience Maintenance Schedule for Operating Systems and Applications ✓ Create an Incident Response Kit ✓ Schedule Quarterly Access Reviews and a Tabletop Exercise on Potential Incidents.

FAQs

1. Do lawyers require Cyber Essentials?

While there is no legal requirement for many law firms, Cyber Essentials is seen as an important baseline and is a requirement for clients and supply chains. The NCSC has explained Cyber Essentials as having 5 technical controls.

2. Is it secure for law firms to work from home?

Typically, yes with encrypted devices, use of MFA, controlled access to systems, and established working-from-home policies.

3. What should you do if your client's email has been breached?

In the event of a breach, you need to consider this an incident: limit access to your account, perform an assessment on what was disclosed, collect evidence, and determine if there are data-breach procedures required. The ICO has a data breach response guideline and a 72-hour deadline on reporting in certain circumstances.

4. When should legal records be destroyed?

The retention schedule for legal records will vary from case to case, by the type of insurance you hold, and your own company policies. It is important to have a written retention policy and to review the policy regularly.

5. **What evidence should law firms maintain post-incident?**

The firm must maintain an incident timeline, actions taken, affected accounts/devices, relevant logs/alerts, decisions made, and lessons learned. All information must be securely maintained.

6. **Does my firm need to encrypt every laptop?**

Generally, yes for the current legal working environment. Encrypting a laptop reduces the chance of having information compromised if it is lost or stolen.

7. **What's a reasonable backup approach?**
   Back up critical data with a plan you can restore from; test restores. Consider how ransomware could affect backups.

8. **How frequently should we engage in security awareness training?**

It is recommended that short and frequent refresher trainings are more effective then one annual long training session. The focus of refresher training should be on identifying phishing and payment diversion attempts.

Final soft CTA

If you would like to have a professional IT health check or risk assessment based on this checklist, a helpful assessment includes:

- Risk associated with identity and administrator access (MFA, privileges, employee separations).
- Email Security and Fraud Protection (DMARC, anti-phishing, verification).
- Document Access Model (e.g. DMS / SharePoint, sharing and permissions).
- Backup and Recovery Testing (e.g. restoring files, ransomware protection).
- Incident Monitoring (e.g. alerting, logging, and first-hour response plan).

A professional assessment will provide you with a prioritised action plan (items that require immediate attention vs. those that do not) and a baseline for measuring security awareness to be completed at least once each quarter.

About This Guide

The **Computer Support Center** created this guide to assist UK-based IT support and managed-service providers (MSPs) working along with small and medium-sized law practices. It was developed from their experience in the daily IT operation, protecting IT security, and preventing risks associated with the legal industry.

Goal of this document is to provide the legal profession with a relatively simple and practical IT building block of which they may have both a solid foundation as well as a way of easily applying that information to their practice without requiring extensive technical background knowledge. The guise's objectives include providing law firms with sensible default security settings, assigning

direct accountability, and reducing common risk elements present in UK legal practices, all while leaving out ambiguity, excessive complexity, and sales-element driven recommendations.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

The foundation of law firm operations, protecting client information, and complying with regulatory requirements is having secure, reliable IT. By focusing on the basic elements – ownership clarity, access authentication, device management, and incident response preparation – law firms can greatly reduce their risk and improve their resiliency.

Ultimately, a checklist like this will help a UK law firm develop a systematic methodology for implementing IT solutions that will assist them in their daily operations as well as facilitate the long-term success of the firm in an ever-increasingly digital world.